NASJONAL
SIKKERHETSMYNDIGHET

TEMARAPPORT
Innsiderisiko

Om NSM og temarapport

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for nasjonal sikkerhet, som omfatter blant annet informasjonssikkerhet, objekt- og infrastruktursikkerhet, digital sikkerhet, og personellsikkerhet. Direktoratet er nasjonal koordinerings-instans for alvorlige dataangrep og andre ikt-sikkerhetshendelser og drifter varslingssystem for digital infrastruktur.

NSM har som oppgave å forebygge, avdekke og motvirke sikkerhetstruende aktivitet mot offentlige og private virksomheter i Norge. I tillegg forvalter NSM sikkerhetsloven på vegne av Justis- og beredskapsdepartementet.

Gjennom årlige åpne produkter gir NSM ut informasjon om risiko og sårbarheter virksomheter bør være kjent med for å kunne drive eget målrettet sikkerhetsarbeid. NSM arrangerer kurs og publiserer veiledere og håndbøker rettet mot virksomheters sikkerhetsarbeid.

NSM publiserer temarapporter som omhandler risiko på spesifikke tematiske områder med utgangspunkt i verdier, trusler og sårbarheter.

Innhold

TEMARAPPORT Innsiderisiko

Design:
Redink

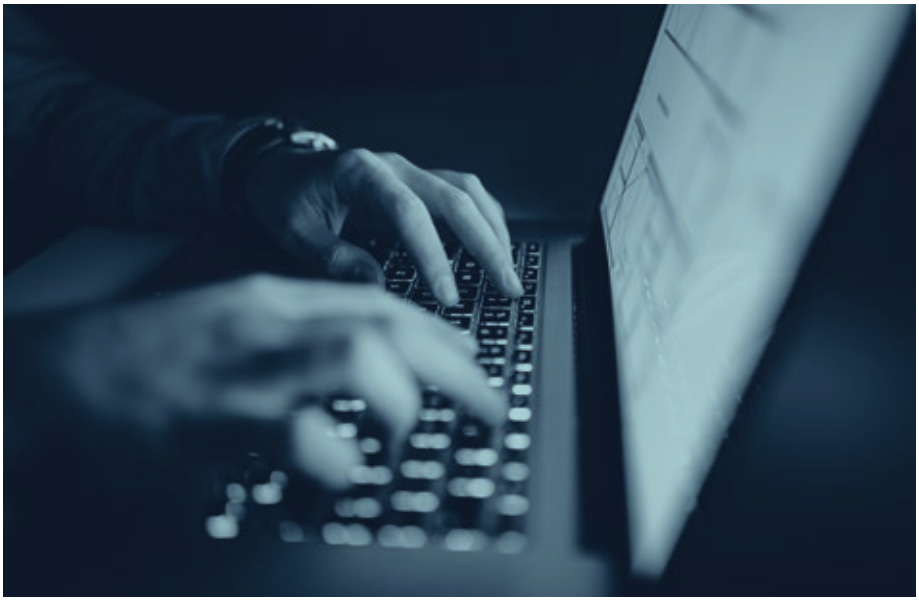
Trykk og distribusjon:
RK grafisk

1

Formål og avgrensing

Formålet med denne temarapporten er å gi leseren en helhetlig forståelse for den potensielle risikoen som er forbundet med innsidevirksomhet. Denne risikoen retter seg mot Norge som stat, offentlige myndigheter, næringslivet og private virksomheter. Dette innebærer at informasjonen i temarapporten er av betydning både i en stats- og samfunnssikkerhetskontekst, men også for private aktører og næringslivet.

Målgruppen for rapporten er både ledere og ansatte i offentlig og private virksomheter . Personell med linjelederansvar, med en rolle i virksomhetens sikkerhetsorganisasjon, eller som gjennom sitt arbeid får tilgang til virksomhetens verdier, er således målgruppen for rapporten. Formålet med rapporten er å øke virksomheter og enkeltpersoners motstandsdyktighet, og gjennom økt kunnskap bidra til at de forebyggende tiltakene virksomheter og organisasjoner implementerer gir god effekt.



2

Bakgrunn

Rapporten omhandler *hva* innsidevirksomhet er og illustrerer hvordan en virksomhet vil kunne være sårbar for denne type aktivitet.

I *Temarapport Innsiderisiko* beskriver NSM risikoen enkeltindivider potensielt utgjør mot Norge som stat eller virksomheter sin informasjon, objekter, infrastruktur eller andre verdier. Virksomheter forstås i denne sammenheng som offentlige forvaltningsorgan eller private virksomheter. Både offentlige og private virksomheter har verdier som må beskyttes. Behovet for beskyttelse av disse verdiene vil variere ut fra hvilken betydning det har for staten eller virksomheten dersom verdien blir utsatt for uønskede handlinger.

Rapporten omhandler *hva* innsidevirksomhet er og *hvordan* en virksomhet vil kunne være sårbar for denne type aktivitet. Informasjonen i rapporten bygger på NSM sin erfaring som fagmyndighet innen personellsikkerhet, samt på åpent tilgjengelig forskningsbasert informasjon og åpne trusselvurderinger fra samarbeidspartnere. Rapporten vil anbefale tiltak som kan iverksettes av virksomhetene for å forebygge, detektere og håndtere innsidevirksomhet.

Hva er en innsider?

Innsiderisikoen virksomheten utsettes for er kompleks og bygger på en rekke ulike faktorerer.

En innsider forstås som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap. Innsideren kjenner virksomhetens rutiner, prosesser og sårbarheter, og kan benytte kunnskapen for å skade virksomheten til fordel for annen virksomhet, stat, eller til egen vinning. Innsideaktivitet kan gjennomføres direkte og på egenhånd, eller på vegne av en ekstern aktør. Eksterne aktører kan være statlige, ikke-statlig eller andre enkeltindivider. Disse aktørene kan søke å utnytte personer med tilgang til en virksomhets eller stats verdier for å oppnå egne mål.

Innsiderisikoen virksomheter utsettes for er kompleks og bygger på en rekke ulike faktorer. Det kan være flere grunner til at en person begår innsidevirksomhet. Vedkommende kan være motivert av egne interesser eller bli påvirket av en ekstern aktør. En ekstern aktør kan ha til hensikt å forlede, rekruttere eller presse en person til å begå innsidevirksomhet. Det forekommer også tilfeller hvor innsideraktivitet begås uten av personen har en klar motivasjon om å gjennomføre dette, men hvor vedkommende gjennom sin adferd utsetter virksomhetens verdier for risiko.

Innsiderisikoen vil være både statisk og dynamisk. Den er statisk ved at det alltid vil eksistere personer på innsiden av virksomheter som vil kunne skade virksomhetens verdier f.eks. ved å kompromittere, sabotere eller manipulere informasjon og prosesser. Innsiderisiko er også dynamisk ved at den ansattes motivasjon, prioritering og lojalitet kan endres. I tillegg kan eventuelle eksterne aktører endre sine mål, modi

Hvem kan innsideren være?

- Personer med direkte tilgang
- Personer som kan skaffe seg tilgang
- Personer som kan påvirke
- Personer med fremtidig potensial
- Personer som kan utnyttes på annen måte, for eksempel gjennom manipulasjon

For å forstå kompleksiteten og variasjonene i innsidevirksomhet, kan risikoen forklares med hjelp av følgende begrep: intensjon, kapasitet og mulighet.

og arbeidsmønstre. Også forhold ved arbeidsplassen påvirker risikoen, f.eks. ved endringer i implementerte sikkerhetstiltak, arbeidsoppgaver, prosesser eller virksomheten for øvrig.

For å forstå kompleksiteten og variasjonene i innsidevirksomhet, kan risikoen forklares med hjelp av følgende begrep: **intensjon**, k**apasitet** og **mulighet**. Dette er variabler som i ulik grad er til stede når innsidevirksomhet oppstår.

Intensjon kan forstås som en persons motivasjon til å gjennomføre en tilsiktet, uønsket handling mo en virksomhets verdier. Intensjon kan oppstå på bakgrunn av en trusselaktør som presser, kultiverer eller overtaler en person til å begå innsidevirksomhet. Trusselaktøren kan ønske å påvirke, styre eller utnytte personens intensjon for å benytte seg av dens tilganger til virksomhetens verdier. I sitt arbeid med å skape intensjon hos personen kan trusselaktøren forsøke å utnytte sårbarheter ved den aktuelle personen. Intensjon om å begå innsidevirksomhet kan også vokse frem som et resultat av personens egne motivasjoner og overbevisninger, uten påvirkning av en ekstern aktør. Hva som motiverer til slike handlinger vil være forskjellig fra person til person, og det er derfor kompetanse- og ressurskrevende å forebygge og oppdage intensjonen bak innsidevirksomhet

Kapasitet kan forstås som summen av kunnskap, tilganger, erfaringer og personlig egnethet en person innehar for å kunne utføre innsidevirksomhet. Kapasitet til å begå innsidevirksomhet vil variere alt etter hvilken aktivitet personen kan utøve uten å vekke mistanke i virksomheten. Personer med administrasjonsrettigheter i informasjonssystemer eller personer som i kraft av sin stilling har tilgang til en stor andel av virksomhetens verdier, kan sies å ha stor kapasitet. Posisjon, plassering og faktisk tilgang er således viktig for vurderingen av en persons kapasitet til å begå innsidevirksomhet. Innsidevirksomhet kan være svært krevende for en person, da det kan ha store personlige konsekvenser og omfatte betydelig hemmelighold. Hvordan enkelt-personer håndterer slike situasjoner vil påvirke individets kapasitet.

Mulighet er den faktiske anledningen en person med intensjon og/eller kapasitet har til å gjennomføre innside-virksomhet. En persons muligheter henger tett sammen med fraværet eller tilstedeværelsen av sikkerhetsmessige tiltak, bevissthet og styring i virksomheten. Dette inkluderer blant annet rutiner og prosesser som er ment å ivareta og sikre virksomhetens verdier.

Handlinger en person med legitim tilgang påfører en virksomhet med resulterende/ påfølgende skade eller tap, kan samlet

sett omtales som innsidevirksomhet. Vedkommende kan ha intensjon om å påføre skade, eller det kan skje uten intensjon. Innsiderne kan således deles inn i ubevisste innsidere og bevisste innsidere.

3.1 Ubevisste innsidere

En ubevisst innsider er en innsider uten intensjon. Det er således en betrodd person med tilgang til en virksomhets verdier eller som tidligere har hatt tilgang, og som uten overlegg påfører virksomheten skade eller tap. Ved denne type innsideaktivitet har personen *kapasitet* og *mulighet*, men variabelen *intensjon* uteblir. Handlinger som begås av ubevisste innsidere henger ofte sammen med **lav sikkerhetsmessig bevissthet hos den aktuelle personen, samt mangelfull sikkerhetsstyring og daglig sikkerhetsmessig ledelse i virksomheten.**

Når en person ubevisst har eksponert eller kompromittert virksomhetens verdier, har det oppstått en situasjon som potensielt vil kunne skape grunnlag for press.

Til tross for at det ikke foreligger intensjon om å begå innsideaktivitet kan resultatet være at personen kompromitterer eller på annen måte skader eller reduserer virksomheten eller statens verdier. Dette kan blant annet skyldes den ansattes manglende kunnskap, naivitet, uoppmerksomhet, manglende bevissthet, eller sviktende kjennskap til sikkerhetsregler og rutiner i virksomheten.

Ubevisst innsideaktivitet **kan også oppstå ved at en trusselaktør forleder, manipulerer eller på annen måte utnytter en person til å begå denne type handlinger.** I slike tilfeller vil den aktuelle personen være angrepsflaten og en kapasitet for trusselaktøren, uten at personen selv er bevisst eller har et ønske om å begå innsidevirksomhet. Eksempler på slike tilfeller av innsidevirksomhet er personer som uten å være klar over det, blir manipulert til å dele informasjon om en virksomhets verdier og sårbarheter med det som viser seg å være en trusselaktør.

Når en person ubevisst har eksponert eller kompromittert virksomhetens verdier, har det oppstått en situasjon som potensielt skaper grunnlag for press. Dette vil kunne utnyttes av trusselaktøren slik at personen gjennomfører ytterligere innsideaktivitet. Frykten for potensielle konsekvenser for personen som har begått den ubevisste handlingen, samt ønsket om å holde dette skjult, kan fungere som et pressmiddel i en slik situasjon. Personen har således blitt en innsider med intensjon til tross for at det i utgangspunktet ikke eksisterte motivasjon for å begå innsidevirksomhet.

3.2 Bevisste innsidere

En bevisst innsider er en innsider med intensjon. Personen er således klar over at vedkommende begår en handling som strider mot virksomhetens interesser. Det er derimot ikke nødvendigvis slik at innsideren i alle sammenhenger er kjent med konsekvensene av handlingene. En handling som for en innsider fremstår som et ufarlig brudd på sikkerhetsrutiner kan i noen tilfeller få store konsekvenser for virksomheten og/eller nasjonal sikkerhetsinteresser.

Intensjonen om å begå innsidevirksomhet kan være **selvmotivert** uten påvirkning av en ekstern trusselaktør. I slike tilfeller vil personen selv ta initiativ til innsidevirksomhet. Dette vil kunne foregå enten ved at personen begår slik aktivitet helt uten involvering av en ekstern aktør, eller ved at personen selv oppsøker aktøren og tilbyr sine tjenester.

Infiltratøren er en person som bevisst søker seg legitim tilgang til en virksomhet og dens verdier med den intensjon om å begå innsidevirksomhet. Infiltratøren kan være direkte knyttet til en fremmed stats etterretningstjeneste eller rekruttert. Trusselaktørens rekruttering av infiltratøren kan enten ha foregått over lang tid, eller gjennom en kort

rekrutteringsprosess. Felles for begge tilnærmingene er at rekrutteringen av infiltratøren alltid vil forekomme før den legitime tilgangen til virksomhetens verdi er etablert.

En innsider kan også være **rekruttert** av en trusselaktør etter at personen har fått tilgang til virksomhetens verdier. En slik person har ikke nødvendigvis i utgangspunktet en intensjon om å bli en innsider. Personen kan derimot bli kultivert, påvirket eller presset av en trusselaktør som ønsker tilgang på en virksomhets verdier. Denne typen innsider kan bevege seg raskt fra å være en lojal ansatt uten intensjon om å skade virksomheten, til å bli en bevisst innsider. Trusselaktøren vil ofte foretrekke å skape en positiv relasjon med en potensiell innsider, der hensikten er å få et forretningsmessig forhold. En slik relasjon vil ofte være mer nyttig for aktøren enn hvor aktøren må bruke press. Dersom press benyttes vil innsideren settes i en vanskelig situasjon og utgjøre en større risiko for aktøren. Samtidig vil trusselaktøren benytte de metodene som er nødvendig for å nå sine mål.

Innsidetrusselen

Det overordnede trusselbildet som til enhver tid møter Norge, har direkte konsekvenser for tilstedeværelsen av innsidevirksomhet. I sine åpne trusselvurderinger har Politiets sikkerhetstjeneste (PST) i flere år pekt på at fremmede stater kontinuerlig forsøker å skaffe seg tilgang til norske beslutninger, strategier og informasjon. PST peker også på at statlige aktører kan komme til å søke innpass i næringslivet, samt i teknologitunge virksomheter og forskningsmiljø.

år statlige aktører ikke makter å skaffe seg denne informasjonen på en legitim måte, kan de forsøke å bruke illegitime midler som f.eks. nettverksoperasjoner, fysiske innbrudd eller rekruttering av innsidere. Dette vil skje i det skjulte for å unngå eventuelle politiske konsekvenser og opprettholde muligheten til plausibel fornektelse. Statlige aktører vil kunne benytte svært inngripende metoder mot virksomheter og enkeltindivider når de er av den oppfatning at dette er i deres interesse.

Hvorfor er innsideren aktuell for en trusselaktør?

Innsideren:

- Kjenner organisasjonen
- Kjenner sikkerhetstiltakene
- Har legal tilgang til systemer/sensitiv informasjon
- Kan manipulere systemer og personer internt
- Kan verifisere informasjon
- Kan operere i det skjulte
- Kan brukes om lang tid/mange år
- Kan utnytte kjente sårbarheter

Hva kan innsideren gjøre?

- Stjele, lekke, offentliggjøre informasjon
- Sabotere (tilgjengelighet, integritet mv.)
- Stjele eller underslå verdier
- Påvirke eller manipulere personer eller systemer
- Hjelpe og tilrettelegge for andre (informasjon, avlytting, bistand til hacking osv.)

På tross av at statlige aktører regnes for å utgjøre størst risiko når det gjelder innsidere, vil også ikke-statlige aktører kunne ha høy kapasitet og svært målrettet intensjon.

Å samarbeide med en statlig trusselaktør vil innebære høy grad av risiko. Aktiviteten vil som regel være ulovlig og samarbeidet med den statlige trusselaktøren kan generelt oppleves å være en vanskelig situasjon for vedkommende. Samarbeidet kan medføre opplevelser av lojalitetskonflikt og stress, samt gi en følelse av at man mister kontroll over egen livssituasjon.

Ifølge PST vil fremmed etterretning fortsette å prioritere rekruttering av enkeltindivider med direkte eller indirekte tilgang til informasjon av interesse for denne type trusselaktør. Statlige trusselaktører har kapasitet til å benytte betydelige ressurser på rekruttering og kultiveringsforsøk av enkeltindivider. Enkelte statlige aktører kan ha et svært langsiktig perspektiv, og aktørene vil kunne jobbe svært målrettet og i det skjulte slik at personen som forsøkes rekruttert ikke selv er klar over det før det er for sent. Statlige trusselaktørers rekruttering av innsidere vil eksempelvis kunne være ledd i å forberede spionasje, sabotasje, eller manipulasjon av beslutningsprosesser eller handlinger.

Også ikke-statlige aktører kan forsøke å rekruttere innsidere eller plassere enkeltindivider på innsiden av en virksomhet for å oppnå egne mål. På tross av at statlige aktører regnes for å utgjøre størst risiko når det gjelder innsidere, vil også ikke-statlige aktører kunne ha høy kapasitet og svært målrettet intensjon. Ikke-statlige aktører kan eksempelvis være motivert av et ønske om økonomisk vinning og industrispionasje. Å rekruttere en person med kjennskap til beslutninger og innflytelse på interne prosesser vil i noen tilfeller være et prioritert mål. Virksomheter og bransjer preget av høy teknologisk, økonomisk eller funksjonell verdi og konkurranse kan bli utsatt for denne type innsideaktivitet. Ikke-statlige aktører vil også kunne motiveres av politisk eller samfunnsmessig overbevisning og forsøke å rekruttere innsidere for å kompromittere eller påvirke beslutninger aktøren er spesielt opptatt av.

Rekrutteringsprosessen

Tilnærming, rekruttering og press er metoder som trusselaktører aktivt benytter for å få tilgang til informasjon gjennom en tredjepart. Før et tilnærmingsforsøk vil trusselaktøren ha kartlagt personens personlighet, motivasjonsfaktorer og sårbarheter. Dette gjøres gjennom innhenting av informasjon via sosiale medier, overvåking eller via andre relevante kilder aktøren har tilgang på.

Når en person blir tilnærmet av en trusselaktør vil vedkommende ofte ikke være klar over dette selv. Det første møtet med en trusselaktør kan eksempelvis skje gjennom kontakt i en arbeidssituasjon, tilsynelatende tilfeldige møter, via sosiale medier eller ved en introduksjon fra en felles bekjent. Tilnærmingen og relasjonsbyggingen vil kunne foregå skjult og bære preg av sosial manipulasjon. Personen som blir tilnærmet vil ofte oppleve å ha kontroll og være del av en trygg situasjon. Trusselaktøren vil ofte ønske å skape et vennskapelig forhold for å kunne rekruttere eller verve personen til å handle eller operere som en innsider uten at det foreligger noen form for press. Hensikten med relasjonsbyggingen er å etablere kontakt og samarbeid som over tid leder til at personen kan fungere som en innsider på vegne av trusselaktøren. For å få til et samarbeid så vil trusselaktøren benytte kultivering og gjøre seg attraktiv og interessant for den potensielle innsideren. Trusselaktøren gjør dette ved å gi personen det den ønsker, enten om det er en samtalepartner, en venn, en kjæreste, økonomisk eller andre former for godtgjørelser.

Dersom vedkommende lar seg overtale og rekrutteres av trusselaktøren så vil forholdet kunne endres over tid til å innebære både trusler og press. Dette er særlig aktuelt dersom den rekrutterte personen begår lovbrudd på vegne av trusselaktøren, for eksempel å lekke informasjon eller på annen måte skade virksomhetens verdier, eller hvis personen har blottlagt egne sårbarheter overfor trusselaktøren. Til tross for at trusselaktøren vil foretrekke et samarbeid tuftet på en positiv relasjon, så vil dette kunne sette personen i en vanskelig situasjon hvor aktøren får mulighet til å yte press mot personen for å opprettholde samarbeidet. I ytterste konsekvens vil trusselaktøren kunne bruke manipulasjon, trusler om vold eller andre sanksjoner for opprettholde samarbeid.

De syv fasene i rekrutteringsprosessen

ARC er en modell som illustrrerer de ulike trinnene en rekrutteringsprosess kan innebære.

1. ANALYSE
Hele rekrutteringsprosessen begynner med en analyse av hva trusselaktøren har behov for. Eksempler på slike behov er tilgang til informasjon, teknologi, påvirkning av beslutningsprosesser, beslutningstakere o.l. Dette vil være styrt av trusselaktørens behov og mål.

2. MÅLSØKING
Analysen danner grunnlag for målsøking. Trusselaktøren vil forsøke å finne en person som har, eller kan få tilgang på informasjonen eller verdiene aktøren søker. Dette kan gjøres ved å hente inn person- og virksomhetsopplysninger via internett, sosiale medier og andre åpne eller lukkede kilder. Dette er opplysninger som aktøren kan bruke til å identifisere og kartlegge potensielle mål for en rekrutteringsoperasjon.

3. STUDIE
Når trusselaktøren har identifisert en person som har eller kan få de tilgangene den har behov for, kartlegges denne personen. Informasjon om vedkommende sine personlige egenskaper, sårbarheter, økonomi, motivasjon, politisk ståsted osv. er blant forholdene som kan vurderes for å avklare om vedkommende er et mulig mål for kultivering eller press.

4. TILNÆRMING
Trusselaktøren tar kontakt med målpersonen. Dette kan f.eks. være et fysisk møte, gjennomføres digitalt eller via en tredjeperson. Tilnærmingen kan bære preg av å være et tilfeldig møte, men vil ofte være planlagt ned til den minste detalj.

5. RELASJONSBYGGING
Er det første møtet vellykket vil trusselaktøren søke å skape et forhold til målpersonen i en relasjonsbyggingsfase. Vedkommende kan utsettes for en sjarmoffensiv og blir tilbudt ulike gaver eller goder. I tillegg kan trusselaktøren gi personen små oppdrag som vil oppleves som en naturlig og legal del av relasjonen. Dette kan eksempelvis innebære utveksling av tilsynelatende ikke-sensitiv informasjon. Denne fasen kan i enkelte tilfeller vare i flere år. Relasjonsbygging vil bidra til å senke målpersonen sin terskel for samarbeid.

6. REKRUTTERING
Dette er en kritisk fase for trusselaktøren. Forsøket på å rekruttere en person kan være vellykket eller mislykket. Hvis målpersonen responderer positivt på rekrutteringen vil samarbeidet formaliseres med f.eks. faste møter og godtgjørelser. Målpersonen vil bli bevisst på at vedkommende er involvert i en form for innsidevirksomhet. Målpersonen vil stort sett aldri fullt ut bli kjent med hvem vedkommende faktisk jobber for da trusselaktøren vil sørge for å holde sin egne faktiske identitet skjult.

7. OPPFØLGING
Etter en vellykket rekruttering vil målpersonen få konkrete oppdrag og bli fulgt opp av trusselaktøren. Innsideren vil følges opp med eksempelvis beskyttelse, overvåkning eller trening til fremtidige oppdrag. Når trusselaktøren vurderer at innsideren ikke kan gi mer informasjon eller ikke lenger fungerer på en tilstrekkelig måte, vil forholdet avsluttes midlertidig eller permanent. Trusselaktøren kan fortsette å følge opp innsideren i lang tid etter et gjennomført oppdrag.

Verdi

Manglende eller fraværende kjennskap til egne verdier utgjør en sårbarhet og skaper et mulighetsrom for en potensiell innsider.

En verdi er en ressurs, som hvis den blir utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen. En virksomhets verdivurdering vil kunne si noe om det skadepotensialet innsidevirksomhet vil utgjøre.

Noen virksomheter forvalter informasjon, informasjonssystemer, objekter og infrastruktur som har betydning for Norges nasjonale sikkerhetsinteresser. Disse verdiene kalles skjermingsverdige verdier. Disse verdiene bidrar til å ivareta Norges suverenitet, territorielle integritet og demokratiske styreform. Kompromittering, sabotasje eller manipulasjon av disse verdiene kan ha en direkte negativ konsekvens for Norges nasjonale sikkerhetsinteresser. Det er naturlig å anta at enkelte statlige trusselaktører vil kunne benytte betydelige ressurser og kapasiteter, eksempelvis innsidere, for å skaffe seg tilgang til disse verdiene. Med bakgrunn i dette reguleres beskyttelse av skjermingsverdige verdier av lov om nasjonal sikkerhet (sikkerhetsloven).

Noen virksomheter forvalter verdier som er av betydning for samfunnet, men som ikke har avgjørende betydning for Norges nasjonale sikkerhetsinteresser. Dette kan allikevel være verdier som vil være av interesse for en trusselaktør. En potensiell innsider kan yte stor skade mot virksomheter som direkte eller indirekte støtter opp om verdier av interesse for samfunnet.

De fleste virksomheter forvalter verdier som først og fremst er av betydning for dem selv. Dette kan eksempelvis være finansielle verdier eller informasjon om forretningsideer, forretningsforbindelser, strategi eller forhandlingsposisjoner. Disse verdiene vil også være viktige å beskytte da skadepotensialet kan være avgjørende for den enkelte virksomhet. Både statlige aktører, kriminelle organisasjoner og enkeltindivider vil kunne ha interesse av å eksempelvis kompromittere, sabotere eller manipulere disse verdiene.

Verdier av betydning for nasjonale sikkerhetsinteresser, samfunnsinteresser eller den enkelte virksomhet kan være av både materiell og ikke-materiell art, og omfatter alt fra virksomhetens rutiner, prosesser, systemer, informasjon, infrastruktur, varemerker, omdømme, patenter mv. Manglende eller fravær av kjennskap til egne verdier utgjør en sårbarhet og skaper et mulighetsrom for en potensiell innsider eller en som fører innsideren. Samtidig er det viktig å huske på at verdiene som en potensiell innsider eller trusselaktør søker tilgang til, kan være noe annet enn hva virksomheten selv har definert å være en verdi. Det er derfor svært viktig at virksomheten foretar en verdivurdering som gir et tilstrekkelig grunnlag for en risikovurdering.

Sårbarheter

Sårbarheter kan utløse selvmotivert innsidevirksomhet eller potensielt bli utnyttet av en trusselaktør. Slike sårbarheter kan være knyttet til enkeltindividet, virksomheten og/eller påvirkes av en rekke andre forhold.

6.1 Menneskelige sårbarheter

Den bakenforliggende intensjonen og motivasjonen for at en person velger å bli en innsider er sammensatt og kompleks. Felles er at det er tilstedeværelse av en eller flere menneskelige sårbarheter. Sårbarhetene kan i seg selv lede til innsidevirksomhet eller bli utnyttet av en trusselaktør ved potensiell tilnærming eller rekrutteringsforsøk.

Ideologiske overbevisninger kan være en motiverende faktor for at personer begår innsidevirksomhet. Ideologisk overbevisning kan etableres, styrkes eller styres av samfunnsendringer og nasjonale eller internasjonale hendelser. Ideologi kan både utgjøre et grunnlag for selvmotivert innsidevirksomhet, samt benyttes av en trusselaktør for å kultivere, overbevise, manipulere eller presse personer til å bli en rekruttert innsider. Fellesnevneren for personer som begår innsidevirksomhet på bakgrunn av ideologi er overbevisningen om at deres meninger, oppfatninger eller opplevelser av en situasjon rettferdiggjør og legitimerer innsidevirksomhet. En ideologisk overbevisning kan gjøre at personer setter sine egne eller likesinnedes vurderinger fremfor regler og rutiner knyttet til ivaretagelsen av virksomhetens verdier.

Lojalitetskonflikt oppstår når en person opplever kryssende interesser. Lojalitet kan ses på som opplevd forpliktelse til å handle på en bestemt måte som springer ut fra et sett med forutbestemte verdier. En person kan ha flere lojaliteter slik at det oppstår konflikt mellom

Case

Ideologisk motivert offiser fra Estland, Hermann Simm (72 år)

Hermann Simm var en høytstående offiser fra Estland som i flere år hadde direkte tilgang til høyt gradert informasjon relatert til NATO. I 2008 ble Simm pågrepet, mistenkt for å ha vært en innsider på vegne av russisk etterretning siden midten av 90-tallet. Simm jobbet mye internasjonalt og det viste seg at han hadde hentet inn informasjon fra en rekke allierte NATO land. Informasjonen overleverte han i det skjulte til sin russiske kildefører.

Bakgrunnen for at Simm valgte å spionere på vegne av russisk etterretning antas å være en ideologisk overbevisning. Simm hadde vokst opp da Estland fortsatt var en del av Sovjetunionen. Russisk etterretning brukte denne tilknytningen og den ideologiske sympatien Simm følte for å overtale han til å samarbeide. På et kritisk tidspunkt ble også personer i Simm sin omgangskrets brukt som del av arbeidet med å rekruttere han. Simm mottok regelmessig trening av sin russiske kildefører og hadde et formalisert samarbeid med russisk etterretning. Etter så lang tid i tjeneste for russisk etterretning forelå det et reelt pressgrunnlag, og Simm hadde få muligheter til å selv avslutte innsideaktiviteten uten storepersonlige konsekvenser. Simm ble dømt for spionasje i 2009.

hvilke interesser og forpliktelser som bør ivaretas. Dersom det er kryssende interesser mellom hva virksomheten ønsker og hva trusselaktøren som personen er lojal mot ønsker, vil personen kunne bli dratt mellom motstridende forpliktelser. Denne lojalitetskonflikten kan trusselaktøren bruke som grunnlag for rekruttering og kultivering for å begå innsidevirksomhet. Trusselaktøren kan også bruke personens lojalitetsfølelse som et pressmiddel gjennom trusler eller sanksjoner. Lojalitetskonflikter vil i noen tilfeller også kunne fungere som en selvmotiverende faktor.

Forhold på arbeidsplassen som oppleves som negative for personen kan være en motiverende faktor som leder til innsidevirksomhet. Dette kan eksempelvis resultere i tilfeller hvor innsidevirksomhet begås som et ledd i å hevne seg mot eller skade virksomheten på bakgrunn av opplevd urettferdighet. Det at arbeidstakeren ikke opplever å bli tilstrekkelig verdsatt, forstått eller sett av kollegaer og ledere, kan utgjøre en sårbarhet. Arbeidstakeren kan eksempelvis oppleve å bli behandlet dårlig på arbeidsplassen, føle seg lite involvert i avgjørelser som påvirker personen direkte, ikke oppleve å få gode tilbakemeldinger fra ledere eller føle seg misforstått eller forbigått i forfremmelsesprosesser. Likeledes kan en ansatt selv forsøke å endre virksomhetsprosesser ved å begå innsidevirksomhet, f.eks. dersom virksomheten skal flytte, foreta nedleggelser eller omstrukturere. Hensikten med innsidevirksomheten i disse tilfellene kan være å skape en debatt for igjen å kunne påvirke virksomheten til å endre beslutningen.

Sårbarheter som knytter seg til forhold på arbeidsplassen vil kunne utnyttes av en trusselaktør i en rekrutteringsprosess eller lede til selvmotivert innsidevirksomhet. Trusselaktører kan forsøke å benytte misnøye rundt en arbeidsplass eller

Case

Innsider drevet av lojalitetskonflikt, Reality Winner (27 år)

Reality Leigh Winner var amerikansk etterretningsoffiser og ble i 2017 pågrepet, mistenkt for å ha lekket gradert informasjon til media. Winner hadde tidligere tjenestegjort en rekke ganger i Midtøsten og slet med posttraumatisk stress. Hun var sterk kritisk til Donald Trump, noe hun hyppig uttalte via sosiale medier.

Med bakgrunn i dette skrev hun ut et gradert dokument relatert til den da pågående etterforskningen av russisk innblanding i det amerikanske valget. Dokumentet sendte hun til en rekke mediehus. Winner var motivert av sin politiske overbevisning. Hennes lojalitet var ikke rettet mot ivaretagelsen av virksomhetens verdier, men mot det hun selv oppfattet å være rettferdig og riktig.

I etterkant av hendelsen har Winner uttalt at hun angrer på handlingene sine og at hennes psykiske helse var en faktor. I 2017 ble hun dømt til fengsel for spionasje.

et konkret ansettelsesforhold som en motivasjonsfaktor for å påvirke og skape intensjon hos en person om å begå innsidevirksomhet. Trusselaktører kan videre bruke personers ønske om anerkjennelse som et virkemiddel i sitt arbeid for å nå sine mål. I noen tilfeller vil eksempelvis personen kunne dele virksomhetssensitive detaljer i samtaler uten å være klar over at vedkommende kommuniserer med en trusselaktør og uten å forstå konsekvensene av en slik samtale.

I flere kjente innsidersaker har **økonomi** vært den bakenforliggende motivasjonen som ledet frem til innsideaktivitet. Økonomiske sårbarheter kan lede til både selvmotivert og rekruttert innsidevirksomhet. En svak økonomi eller et ønske om å bli gjeldfri, kan motivere til innsideaktivitet. Selv en person med en stabil økonomi vil kunne motiveres av tilbud om økonomiske fordeler. En innsider som i utgangspunktet er motivert av andre faktorer, vil også kunne motiveres ytterligere av økonomisk kompensasjon fra en trusselaktør for å fortsette eller intensivere allerede pågående innsidevirksomhet.

Endring i livssituasjon, plutselig eller gradvis over tid, har ved flere tilfeller ført til innsidevirksomhet eller vært en indikator på pågående innsidevirksomhet. Plutselige endringer som skilsmisse, sykdom, dødsfall eller andre livshendelser som oppleves traumatiserende og vanskelig, er eksempler på livssituasjoner som kan skape sårbarheter og lede til både bevisst og ubevisst innsidevirksomhet. Endring i livssituasjon kan også aktualisere, svekke eller styrke andre sårbarheter personen har. Sårbarheter knyttet til ustabil eller endret livssituasjon vil videre kunne være

Case

Innsideaktivitet med bakgrunn i arbeidsplassrelaterte forhold, Bradley Manning (31 år)

Bradley Manning jobbet som etterretningsanalytiker i USA da han i 2010 blepågrepet, mistenkt for om å ha lekket gradert informasjon til WikiLeaks.

Manning hadde opplevd mobbing på arbeidsplassen og at hans nærmeste ledere ikke håndterte disse forholdene på en tilstrekkelig god nok måte. Manning hadde også utviklet en politisk overbevisning som gikk på tvers av ivaretagelsen av den graderte informasjonen han hadde tilgang på. Disse overbevisningene kombinert med frustrasjon over egen arbeidsplass var tilstrekkelig til at Manning selv tok kontakt med Wikileaks for å tilby sine tjenester som en innsider.

Wikileaks brukte lang tid på å gi Manning den treningen han trengte for å kunne handle uoppdaget som en innsider. Manning hadde administrasjonsrettigheter i IT-systemene han jobbet på og kunne derfor tilegne seg informasjon som han i utgangspunktet ikke skulle ha tilgang på. Dette bidro til at Manning lekket svært store mengder med informasjon. Manning benyttet en minnepinne for å frakte informasjonen uoppdaget ut av virksomheten sin. Etter selve hendelsen gikk det ikke lang tid før Manning ble oppdaget. Manning ble dømt for spionasje i 2013.

Lav eller manglende sikkerhetsmessig bevissthet vil øke risikoen for at personer kan kompromittere sensitiv informasjon og bli ubevisste innsidere.

noe en trusselaktør forsøker å utnytte for å kultivere eller presse personen til å bli en innsider. Trusselaktøren kan forsøke å overbevise personen til å tro at de kan hjelpe vedkommende ut av en vanskelig situasjon dersom han eller hun blir en innsider, eller true personen med å offentliggjøre endringen i livssituasjonen.

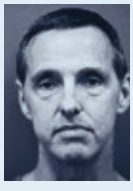
Manglende eller lav sikkerhetsmessig bevissthet kan i seg selv utgjøre en sårbarhet. Sikkerhetsmessig bevissthet anses som viljen og evnen til å håndtere virksomhetens verdier i tråd med gitte retningslinjer og regelverk. Lav eller manglende sikkerhetsmessig bevissthet øker risikoen for at personer med tilgang kan kompromittere sensitiv informasjon og bli ubevisste innsidere. I kombinasjon med andre sårbarheter kan manglende eller lav sikkerhetsmessig bevissthet øke risikoen for innsidevirksomhet og gjøre at personer blir mer sårbare for tilnærming og kultivering fra trusselaktører.

6.2 Virksomhetsspesifikke sårbarheter

Også virksomhetsspesifikke sårbarheter kan i noen tilfeller påvirke risikoen for innsidevirksomhet. Sentralt her er **tilstedeværelse eller fravær av sikkerhetsstyring**. Manglende rutiner, manglende prosedyrer og manglende styringsdokumenter for sikkerhet skaper økt mulighetsrom for en potensiell innsider og reduserer virksomhetens deteksjonsevne. I de tilfeller hvor virksomheter forsømmer ansvaret sitt knyttet til daglig oppfølging av ansatte og nedprioriterer sikkerhetsmessig ledelse vil virksomhetsspesifikke sårbarheter kunne oppstå. **Utilstrekkelig oppfølging av virksomhetens ansatte** utgjør en betydelig risiko ved at sårbarheter ikke blir oppdaget eller håndtert. Manglende ledelsesforankring av sikkerhet, lav risikoforståelse eller mangelfull kompetanse reduserer

Case

Økonomisk motivert innsider med tilknytning til Kina, Kevin Mallory (62 år)



I 2017 ble den tidligere etterretningsoffiseren Kevin Mallory arrestert og mistenkt for spionasje på vegne av kinesisk etterretning.

Mallory hadde noen år tidligere sluttet som amerikansk etterretningsoffiser og startet sitt eget firma. Dette firmaet slet økonomisk, og det samme gjalt Mallory personlig. Via LinkedIn ble Mallory kontaktet av en person som utga seg for å jobbe for en kinesisk tenketank. Personen ønsket å ansatte Mallory og inviterte han til Kina. Etter en relasjonsbyggingsfase ble Mallory rekruttert etter løfter om økonomiske godtgjørelser. I etterkant har det vist seg at personen var en kinesisk etterretningsagent. Agenten ga Mallory opplæring og en kryptert telefon slik at de kunne holde kontakt.

Mallory hadde i sin tidligere jobb hatt tilgang til svært sensitiv informasjon. Mallory hadde overlevert det han selv hadde tilgang til, tok han kontakt med en rekke tidligere kollegaer og forsøkte å hente inn ytterligere informasjon fra dem. En av de han tok kontakt med ble mistenksom, og det ble etter hvert åpnet en etterforskning. Mallory ble dømt for spionasje i 2019.

barrierer som er ment å avdekke og forhindre innsidevirksomhet. NSM har over tid observert flere tilfeller hvor sikkerhetsbevisstheten og sikkerhets-oppfølgingen av ansatte avtar over tid, parallelt med at ansettelsesforholdet modnes. Dette er en sårbarhet og øker risikoen virksomheten utsettes for.

Den interne **sikkerhetskulturen** i en virksomhet vil være avgjørende for å forebygge og oppdage innsidevirksomhet. Sikkerhetskultur handler om adferd knyttet til sikkerhet. Det er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd. Sikkerhetstruende adferd og hendelser er ofte et resultat av usunn sikkerhetskultur innad i virksomheten. Dette kan skyldes manglende kunnskap og evne til å foreta riktige beslutninger, eller være handlinger hvor noen bevisst velger å omgå sikkerhetsrutiner og prosesser. Fraværet av en hensiktsmessig sikkerhetskultur og lav bevissthet blant de ansatte kan utnyttes av trusselaktører, og vil også kunne føre til hendige uhell ved at personer kan agere som ubevisste innsidere.

Ulik eller manglende risikoforståelse vil også kunne utgjøre en sårbarhet. En slik sårbarhet kan ofte skyldes at virksomheten ikke har etablert en felles risikoforståelse som er tilpasset den faktiske innsidetrusselen virksomheten står overfor. Dersom behovet for rask rekruttering av kompetent personell trumfer hensynet til personellsikkerhet, påfører virksomheten seg potensielt økt risiko. F.eks. vil en slik prosess kunne føre til at eventuelle menneskelige sårbarheter ikke vurderes tilstrekkelig og at virksomheten ikke blir bevisst på risikoen de utsetter seg for ved å ansette personen. Det kan også føre til at den aktuelle personen ikke får tilstrekkelig sikkerhetsfaglig opplæring og at risikoen for ubevisst innsidevirksomhet øker.

Hvilke verdier en virksomhet besitter vil utgjøre grunnlaget for hva som må beskyttes mot eventuelle

innsidere. **Kartlegging av verdier og risikovurderinger** der man får tydeliggjort hvilken risiko den konkrete virksomheten står overfor er avgjørende for å redusere virksomhetens sårbarhetsflate. Ved manglende verdivurdering vil det oppstå risiko for at informasjon tilgjengeliggjøres for potensielle innsidere og trusselaktører.

Fysisk sikring er grunnleggende sikringstiltak for å hindre uvedkommende fysisk tilgang til virksomhetens informasjon og verdier. I tillegg til å holde utenforstående borte fra virksomhetens verdier vil det i noen tilfeller være nødvendig å etablere fysiske barrierer og adgangskontroll som regulerer og kontrollerer egne ansattes tilganger. **Soneinndeling** som sørger for at kun autorisert personell kan ha fysisk tilgang til gitte områder, vil redusere mulighetsrommet til en potensiell innsider. Fravær eller dårlig oppfølging av en virksomhets adgangskontrollsystemer utgjør en betydelig sårbarhet. Dersom virksomheten ikke har klart definert hvilket personell som skal ha fysisk eller logisk tilgang til et område vil dette medføre redusert kontroll og utgjøre en sårbarhet som kan øke innsiderisikoen.

I tillegg til at en virksomhets fysiske sårbarheter påvirker innsiderisikoen, så kan også **logiske og ikt relaterte sårbarheter** få en slik effekt. Digitalisering av samfunnet og virksomheters informasjonssystemer medfører at et økende antall verdier kobles sammen. Dette har i flere tilfeller ført til lange og uoversiktlige verdikjeder og til at enkeltindivider har legitim tilgang til store deler av virksomhetens verdier via informasjonssystemene. Digitale sårbarheter vil således kunne påvirke det samlede mulighetsrommet og kapasiteten til en potensiell innsider og derav risikoen en virksomhet utsettes for.

Case

Potensiell innsidevirksomhet med bakgrunn i ulik risikoforståelse

I 2015 ble en kinesisk og eniransk statsborger utvist av Norge, begge var mistenkt for å gjennomføre spionasje på vegne av fremmed stat. Personene var ansatt ved et universitet i Norge og mottok økonomisk støtte til forskningen sin. De hadde i tillegg tilknytning til et kinesisk forskningsinstitutt. Det har senere vist seg at dette instituttet var falskt og forbundet med kinesisk etterretning.

Norske myndigheter avdekket at forskningen kunne brukes som ledd i utvikling av hypersoniske missiler. Forskningen og kunnskapen personene tilegnet seg i Norge ville således kunne brukes av en fremmed stat til militære formål.

I etterkant av at disse personene ble utvist har det vært offentlig uenighet om hvorvidt anklagene var legitime og et tilstrekkelig grunnlag for utvisning. Fra et innsideperspektiv kan det sies å ha vært ulik risikoforståelse hos det aktuelle universitetet som muliggjorde forskningen og norske myndigheter. Forskningen ville kunne få konsekvenser for norske nasjonale sikkerhetsinteresser, og at forskerne hadde legitim tilgang til type informasjon utgjorde en innsiderisiko.

En sentralt plassert innsider kan være et svært effektivt virkemiddel for å oppnå målet om å kompromittere en virksomhets nettverk og informasjonssystemer dersom disse ikke er tilstrekkelig sikret. Dersom virksomhetens informasjonssystem ikke er konfigurert på en sikkerhetsmessig god måte så vil dette i en innsidesammenheng kunne utgjøre en sårbarhet. Dersom en virksomhet tillater at et høyt antall ansatte har administrasjonsrettigheter øker mulighetsrommet til innsideren betraktelig. Administrasjonsrettigheter vil blant annet gi innsideren mulighet til å innføre og ta i bruk spesialiserte verktøy andre ikke har. Administrasjonsrettigheter vil videre gjøre avdekking av pågående innsideaktivitet vanskeligere ved at innsideren kan slette sporene etter seg. Flate nettverksstrukturer med fravær av logisk informasjonssegregering kan muliggjøre at en innsider beveger seg fritt i informasjonssystemet og kompromitterer større deler av virksomhetens verdier og infrastruktur.

Fraværende eller mangelfull logging i virksomhetens informasjonssystemer kan utgjøre en sårbarhet som påvirker evnen til å avdekke pågående innsideaktivitet. Fravær av automatiserte prosesser for vedlikehold og sikkerhetsoppdateringer øker de digitale sårbarhetene som en potensiell innsider kan utnytte. Manglende styring av hvilken maskin- og programvare som tillates brukt på virksomhetens informasjonssystemer øker mulighetsrommet til en potensiell innsider og påvirker virksomhetens sårbarhetsflate. Logiske sårbarheter øker mulighetsrommet til en potensiell innsider og reduserer risikoen som innsideren potensielt må utsette seg selv for.

6.3 Andre sårbarheter

Også andre sårbarheter enn det som er av menneskelig og virksomhetsspesifikk art vil kunne påvirke hvorvidt innside-virksomhet oppstår og aktualiseres. Det er derfor viktig å ha en helhetlig tilnærming til sårbarhets- og risikobildet.

Case

Ubevisst innsidevirksomhet muliggjort pga. virksomhetsspesifikke sårbarheter

I 2018 ble en person i en norsk ikt-virksomhet det som kan sies å være en ubevisst innsider.

Personen hadde ansvar for overvåking av et serverrom. Dette rommet inneholdt sensitiv driftskritisk informasjon. For å overvåke serverrommet satte vedkommende opp et kamera som kontinuerlig sendte oppdaterte stillbilder tilbake til vedkommende sin personlige hjemmeside. Hjemmesiden var offentlig tilgjengelig og alle hadde mulighet til å koble seg til dette kamera for å se live-oppdateringer fra det aktuelle serverrommet.

Intensjonen til personen var å sørge for at serverrommet var sikret, men den utilsiktede konsekvensen var at sensitiv informasjon ble tilgjengelig på internett. Personen ønsket ikke å agere som en innsider og handlingen var således ubevisst. Bakgrunnen for at dette kunne oppstå var manglende sikkerhetsstyring i virksomheten som tillot at dette skjedde.

Ved å forske på kjente innsidesaker har man blant annet funnet at samfunnsendringer, befolkningssammensetning, samt lokale og globale politiske svingninger vil kunne påvirke hvem som blir en innsider.

Ved å forske på kjente innsidesaker har man blant annet funnet at **samfunnsendringer**, befolknings-sammensetning, samt lokale og globale politiske svingninger kan påvirke hvem som blir en innsider. Ofte henger disse momentene sammen med at personers opplevelse av lojalitet påvirkes av en rekke eksterne variabler. Geopolitiske endringer som skaper engasjement og tydeligere politiske skillelinjer, vil kunne være drivende for å skape lojalitetskonflikter hos enkeltindivider og ideologisk motivert innsidevirksomhet.

Andre faktor som kan fungere som sårbarhet i en innsidesammenheng er **teknologisk utvikling**, samfunnets økte ikt-avhengighet og fokuset på digitalisering av funksjoner og informasjon. Dette er trender som gir økt antall personer tilgang på informasjon og verdier, og som øker mulighetsrommet til potensielle innsidere. Utstrakt bruk av sosiale medier fører til at trusselaktører i større grad kommer i kontakt med potensielle målpersoner. Sosiale medier kan derfor fungere som en plattform som trusselaktører kan benytte for å forme lojalitetsbånd, kultivering og oppfølging av innsidere.

Innsiderisiko

For å forebygge innsidevirksomhet vil virksomheter måtte ha en helhetlig tilnærming til forebyggende sikkerhet som ivaretar både de fysiske, logiske og personellmessige aspektene ved sikkerhet.

Det vil alltid foreligge en grad av risiko og usikkerhet knyttet til innsideproblematikk. Det er derfor viktig å håndtere risikoen knyttet til personer ansatt i virksomheten både før, under og etter ansettelsesforholdet.

Risikoen for at virksomheter utsettes for innsideaktivitet oppstår med bakgrunn i (i) verdiene virksomheten eller staten forvalter, (ii) en kombinasjon av menneskelige, virksomhetsspesifikke og/eller andre sårbarheter, og (iii) det overordnede trusselbildet som til enhver tid møter Norge og den aktuelle virksomheten.

Innsidevirksomhet mot Norges nasjonale sikkerhetsinteresser vil ha alvorlige konsekvenser. En innsider med eller uten intensjon kan påføre en virksomhet store skader, blant annet ved å svekke eller fullt ut eliminere fysiske og logiske sikkerhetsbarrierer.

Innsidetrusselen eksisterer uavhengig av om virksomheten forvalter verdier av betydning for stat, samfunn eller kun den aktuelle virksomheten. Graden av risiko dette innebærer vil være både være tett knyttet opp mot tilstedeværelsen eller fraværet av menneskelige og virksomhetsspesifikke sårbarheter og være avhengig av graden av personens og virksomhetens sikkerhetsmessige bevissthet.

Risiko må vurderes ut fra den enkelte virksomhets behov, men også ut fra samfunnet sine behov som helhet. Virksomheter må kjenne sine egne verdier og sårbarheter slik at de er bevisste på den faktiske risikoen de utsettes for. Risikobildet tilsier også at virksomheter både må lære seg å håndtere og leve med en grad av risiko og usikkerhet.

Risikoreduserende tiltak

For å redusere risiko knyttet til innsidevirksomhet kan virksomheter iverksette en rekke tiltak som vil bidra til å forbygge, avdekke og på annen måte motvirke innsidetrusselen.

Skap et helhetlig system for å styrke personellsikkerheten

For å redusere risiko er det avgjørende at virksomheter skaper et helhetlig system for ivaretakelse av personellsikkerhet. Et slikt system bør være integrert i virksomhetens helhetlig styringssystem for sikkerhet. Helhetlig personellsikkerhetsarbeid innebærer å vurdere den menneskelige faktoren i alle deler av sikkerhetsarbeidet og innarbeide mulige konsekvenser av innsidevirksomhet i den totale risikovurderingen. Forankring i ledelsen, tydeliggjøring av ansvar, og utarbeidelse av rutiner og retningslinjer, er tiltak som kan bidra til å styrke personellsikkerheten i virksomheten. Dette bør fortrinnsvis gjøres som en integrert del av virksomhetens system for sikkerhetsstyring, men kan også gjøres som en frittstående oppgave.

Ivareta personellsikkerheten før, under og etter ansettelse

For å motvirke innsidetrusselen bør virksomheten sikre at risikoreduserende tiltak ivaretas i alle ledd av ansettelsesprosessen. Bakgrunnssjekk av kandidater er et tiltak som kan forhindre feilansettelser og eventuell fremtidig innsidevirksomhet. Bruk av bakgrunnssjekker bør alltid tilpasses virksomhetens behov, muligheter og begrensninger.

Etter en ansettelse kan sikkerhetsmessig oppfølging av den enkelte bidra til at virksomheten avdekker sårbarheter og identifiserer tiltak som kan redusere risiko. Autorisasjonsskiller og/eller soneinndelinger er tiltak som vil være risikoreduserende opp mot innsidevirksomhet. Videre vil implementering av tiltak rettet mot ansatte som har nøkkelfunksjoner eller særlig omfattende tilgang til virksomhetens verdier være med på å redusere risikoen for innsidevirksomhet. Ved avslutning av ansettelsesforholdet bør virksomheten alltid gjennomføre tiltak som reduserer den ansattes muligheter til å skade virksomheten i ettertid.

Sørg for at virksomheten har tilstrekkelig kompetanse og ressurser

Tilstrekkelig kompetanse og ressurser er nødvendig for å kunne beskytte en virksomhets verdier mot innsidevirksomhet. Dette er også

nødvendig for at virksomheten skal settes i stand til å følge opp sårbarheter som oppstår hos ansatte. Både virksomhetens ledere, mellomledere og ansatte bør gjøres kjent med det aktuelle risikobildet og mulige indikatorer på innsidevirksomhet. For at kompetansehevende tiltak skal ha en reell risikoreduserende effekt, bør det settes av tilstrekkelig med ressurser for å sikre at kunnskap om personellsikkerhet holdes ved like, utvikles og anvendes.

Legg til rette for en god sikkerhetskultur

Det å legge til rette for en god sikkerhetskultur handler om gjøre personellsikkerhet til en naturlig del av virksomheten. Det er virksomhetens leder sitt ansvar at sikkerhetskulturen er god, og det er derfor viktig at lederen går foran som et godt eksempel. En god sikkerhetskultur bør blant annet ta sikte på å øke ansattes forståelse av sikkerhetsregler og rutiner, samt tilrettelegge for oppfølging av de ansatte for å avdekke misnøye eller andre forhold. Tiltak som kan bidra til dette er belønning av positiv sikkerhetsatferd blant ansatte, jevnlige kampanjer for å øke ansattes bevissthet og en god tilbakemeldingskultur.

Håndter hendelser, evaluer tiltak og lær av erfaringene

Ved sikkerhetsbrudd bør virksomheten identifisere hvilken rolle personen på innsiden har hatt, også i hendelser av en mer teknisk art. Virksomheten bør arbeide systematisk for å lære av erfaringene, og å bruke lærdommen til å styrke arbeidet med å forebygge, avdekke og motvirke innsidevirksomhet.

Les mer om forebygging av innsidevirksomhet

NSM gir ut veiledningsmateriale som retter seg både mot virksomheter underlagt sikkerhetsloven og virksomheter utenfor sikkerhetslovens domene. Disse produktene bør konsulteres i forbindelse med virksomheter sitt arbeid med å redusere innsiderisiko. Dette er eksempelvis:

- Grunnprinsipper for personellsikkerhet
- Håndbok i autorisasjon og daglig sikkerhetsmessig ledelse
- Veileder for personellsikkerhet
- Sikkerhet ved ansettelsesforhold

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814
1306 Sandvika

post@nsm.stat.no
www.nsm.stat.no